Efficient and Secure Data Transfer in Group and Subgroups With Frequent Change in Membership

(ESDT-FCM)

Geetha.M, M.Tech CSE,
Dept. of Computer Science,
M.S.Engineering College,
Navarathna Agrahara,Sadahalli P.O., Bangalore-562 110
Geethaneha5@gmail.com

***Abstract*— Cloud computing is the one which provides an efficient solution for sharing group resources among all the cloud users.So,sharing data in a multi-owner manner while preserving data privacy and identity privacy from an untrusted cloud has posed a challenging issue, due to the frequent change of the memberships. This paper proposes a efficient and secure multiowner data sharing scheme for dynamic groups in the cloud. By leveraging group signature and dynamic broadcast encryption techniques, any cloud user can anonymously share data with others. Meanwhile, the storage overhead and encryption computation cost of this scheme are independent with the number of revoked users. In addition, it takes analyzing the security of our scheme with rigorous proofs, and demonstrate the efficiency of this scheme in experiments**

***Keywords*—Cloud computing, data sharing, privacy-preserving, access control, dynamic groups**

1 INTRODUCTION

One of the most fundamental services offered by cloud providers is data storage. Let us consider a practical data application. A company allows its staffs in the same group or department to store and share files in the cloud. By utilizing the cloud, the staffs can be completely released from the troublesome local data storage and maintenance. However, it also poses a significant risk to the confidentiality of those stored files. Specifically, the cloud servers managed by cloud providers are not fully trusted by users while the data files stored in the cloud may be sensitive and confidential, such as business plans. To preserve data privacy, a basic solution is to encrypt data files, and then upload the encrypted data into the cloud.

2 RELATED WORK

Kallahalla et al. proposed a cryptographic storage system that enables secure file sharing on untrusted servers, named Plutus. By dividing files into filegroups and encrypting each filegroup with a unique file-block key, the data owner can share the filegroups with others through delivering the corresponding lockbox key, where the lockbox key is used to encrypt the file-block keys. However, it brings about a heavy key distribution overhead for large-scale file sharing. Additionally, the file-block key needs to be updated and distributed again for a user revocation

In [3], KP-ABE technique has been used. The file was encrypted using the random key by the data owner; further random keys are encrypted using the set of attributes using KP-ABE.When the group manager assigns an access structure and the corresponding secret key to the user, user can only decrypt the cipher text if and only if the data file attributes satisfy the access structure.

In [5], there are 2 parts in the file which is stored on the untrusted server file metadata and the file data. The file metadata consists of the access control information. But here the user revocation is intractable for large-scale data sharing, because the file metadata has to be updated very frequently.

In [6], all the blocks of contents were encrypted using symmetric content keys by the data owner of data. The public key was used to encrypt again these content keys. For access control, proxy cryptography is used by the server to directly reencrypt the content keys. But the problem was collusion attack between the malicious user and the untrusted server can be happen through which it is possible to learn the decryption keys of all the encrypted blocks.

3 PROPOSED SYSTEM

To solve the challenges for dynamic groups in the cloud. The main contributions of this schema include

1. It propose a secure multi-owner data sharing scheme with user in the group can securely share data with others by the untrusted cloud.
2. This proposed scheme is able to support dynamic groups efficiently.
3. It provides secure and privacy-preserving access control to users, which guarantees any member in a group to anonymously utilize the cloud resource.
4. It provides rigorous security analysis, and perform extensive simulations to demonstrate the efficiency of our scheme in terms of storage and computation overhead.

4 SYSTEM ARCHITECTURE

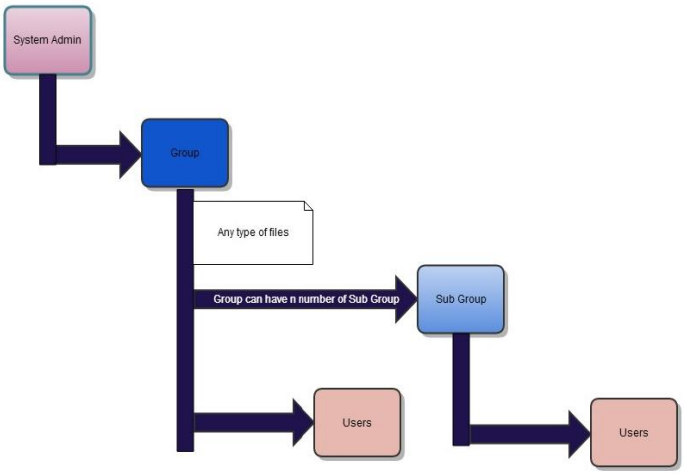

Fig.4.1 System Architecture

5 MODULES AND ITS DESCRIPTION

1. Login Process
2. Group and Sub Group creation
3. User creation
4. File uploading and various operation with file
5. User permission management

1. Login Process:

There is no user while system is installed on server. By default one system user will be created who will be responsible for Group and User creation. System user can only create Group and User. Access permission between Group, Subgroups and Users shall be done by Group admin only. System admin and Group admin can upload any files. File uploaded by System users can visible to all Groups and Subgroup. But file uploaded by Group admin can visible to only his group and sub group. Group admin can give permission to user who can access files.

2.Group And Subgroup Creation:

Group shall be created by System admin, however Subgroup need to create by Group admin only. System admin cannot create Subgroup.

While creating a subgroup, user needs to enter email id and same need to verify. After verification of email id only private access key will be generated which will be sent to Group admin's email address.

To generate access key , group admin user need to enter his secrete key which can be used incase if group admin user forgot his access key. Generated access key will sent by email to Group admin user.

3.User Creation:

User shall be created by System admin only. However access permission to group will be given by Group admin only. User shall be created same way as Group and Sub Group creation.

4. File Uploading And Various Operation With File:

It's a key module of proposed technique. Aim of this module is to grant various permission with files to Group,Sub group and user.Any uploaded file having permission,

1) Read
2) Write
3) Delete

Here, Group admin need to assign each file to user/sub group to whom he/she wanted to give type of access. Based on type of access of file to user, he/she can do various file operation.

5.Permission Management:

Permission will be given by Group admin to user. Each user is having a Private key as well as Access key.

1) *Private Key:* Generated while user creation. It's a unique key across all users, generate by user name, user created time and users secrete key . Also java's MD5 algorithm shall be used to create Private key.
2) *Access Key:* its dynamic key varies based on user's private key and access right on file.(User's access right: Files of which group and sub group user can access with what type of file access).
3) Once Group admin add any file to user with some file right, access key of the user will be changed.
4) Basically, access key will have information of user access. i.e which file of which Group with which type of file permission.
5) Once user removed from any of file access right, access key will changed.

6 CONCLUSION

In this paper, it has a design to secure the data sharing scheme for dynamic groups in an untrusted cloud. Here a user is able to share data with others in the group without
revealing identity privacy to the cloud.
This scheme supports efficient user revocation and new user joining.Moreover, the storage overhead and the encryption computation cost are constant.In Enhancement level is planned to work on sub group level also.

7 REFERENCES

[1] M. Armbrust, A. Fox, R. Griffith, A.D. Joseph, R.H. Katz, A. Konwinski, G. Lee, D.A. Patterson, A. Rabkin, I. Stoica, and M. Zaharia, "A View of Cloud Computing," Comm. ACM, vol. 53, no. 4, pp. 50-58, Apr. 2010.

[2] S. Kamara and K. Lauter, "Cryptographic Cloud Storage," Proc. Int'l Conf. Financial Cryptography and Data Security (FC), pp. 136- 149, Jan. 2010.

[3] S. Yu, C. Wang, K. Ren, and W. Lou, "Achieving Secure, Scalable, and Fine-Grained Data Access Control in Cloud Computing," Proc. IEEE INFOCOM, pp. 534-542, 2010.

[4] M. Kallahalla, E. Riedel, R. Swaminathan, Q. Wang, and K. Fu, "Plutus: Scalable Secure File Sharing on Untrusted Storage," Proc. USENIX Conf. File and Storage Technologies, pp. 29-42, 2003.

[5] E. Goh, H. Shacham, N. Modadugu, and D. Boneh, "Sirius: Securing Remote Untrusted Storage," Proc. Network and Distributed Systems Security Symp. (NDSS), pp. 131-145, 2003.

[6] G. Ateniese, K. Fu, M. Green, and S. Hohenberger, "Improved Proxy Re-Encryption Schemes with Applications to Secure

Distributed Storage," Proc. Network and Distributed Systems Security Symp. (NDSS), pp. 29-43, 2005.

[7] R. Lu, X. Lin, X. Liang, and X. Shen, "Secure Provenance: The Essential of Bread and Butter of Data Forensics in Cloud Computing," Proc. ACM Symp. Information, Computer and Comm. Security, pp. 282-292, 2010.

[8] B. Waters, "Ciphertext-Policy Attribute-Based Encryption: An Expressive, Efficient, and Provably Secure Realization," Proc. Int'l Conf. Practice and Theory in Public Key Cryptography Conf. Public Key Cryptography, http://eprint.iacr.org/2008/290.pdf, 2008.

[9] V. Goyal, O. Pandey, A. Sahai, and B. Waters, "Attribute-Based Encryption for Fine-Grained Access Control of Encrypted Data," Proc. ACM Conf. Computer and Comm. Security (CCS), pp. 89-98, 2006.

[10] D. Naor, M. Naor, and J.B. Lotspiech, "Revocation and Tracing Schemes for Stateless Receivers," Proc. Ann. Int'l Cryptology Conf. Advances in Cryptology (CRYPTO), pp. 41-62, 2001.